Final Report

Title: Quantum Error Correction

Contract Number: FA5209-04-P-0228

AFOSR/AOARD Reference Number: AOARD-044-010

AFOSR/AOARD Program Manager: Tae-Woo Park, Ph.D.

Period of Performance: 04 Mar. 2004 – 03 Mar. 2005

Submission Date: 06 Jul. 2005

PI: Dong Pyo Chi, Prof.
School of Mathematical Science
Seoul National University
Seoul 151-742, Korea

CoPI: Jinsoo Kim, Prof.
School of Electrical Engineering and Computer Science
Seoul National University
Seoul 151-744, Korea

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
27 JUL 2006	**Final Report (Technical)**	**23-03-2004 to 23-06-2005**

4. TITLE AND SUBTITLE
Quantum Error Correction (QEC)

5a. CONTRACT NUMBER
FA520904P0228

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dong Pyo Chi

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Seoul National Universiy,San 56-1, Shillim-dong, Kwanak-gu,Seoul 151-742,KE,151-742

8. PERFORMING ORGANIZATION REPORT NUMBER
AOARD-044010

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
The US Resarch Labolatory, AOARD/AFOSR, Unit 45002, APO, AP, 96337-5002

10. SPONSOR/MONITOR'S ACRONYM(S)
AOARD/AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AOARD-044010

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

We consider quantum error-correcting codes over alphabets of arbitrary size. We generalize quantum stabilizer codes and develop Calderbank-Shor-Steane construction over quantum systems of arbitrary dimensions using the group structure of alphabets. We also develop a methodology systematically conjoining error-correcting codes into a new class of error-correcting codes. With the help of these methods we give several ways to construct quantum maximum distance separable (MDS) codes and present many families of quantum MDS codes.

15. SUBJECT TERMS
Quantum Information Science, Quantum Algorithms, Quantum Cryptography

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**27**	

1. Abstract

We consider quantum error-correcting codes over alphabets of arbitrary size. We generalize quantum stabilizer codes and develop Calderbank-Shor-Steane construction over quantum systems of arbitrary dimensions using the group structure of alphabets. We also develop a methodology systematically conjoining error-correcting codes into a new class of error-correcting codes. With the help of these methods we give several ways to construct quantum maximum distance separable (MDS) codes and present many families of quantum MDS codes with parameters $[[p^m+a,k,\frac{1}{2}(p^m+a-k+2)]]_{p^m}$, $[[p^{2c}-s,k,\frac{1}{2}(p^{2c}-s-k+2)]]_{p^m}$ for some $-1\le s\le p^{2c}$ and $c\,|\,m$, $[[p^{2m/3}-s,k,\frac{1}{2}(p^{2m/3}-s-k+2)]]_{p^m}$ for some $-1\le s\le p^{2m/3}$, $[[p^c+a,k,\frac{1}{2}(p^c+a-k+2)]]_{p^m}$ for some $c\le m$, $[[n=p_j{}^{m_j}+a_j,k,\frac{1}{2}(n-k+2)]]_{\prod p_j^{m_j}}$, and so forth, where p and p_j are primes, q is a positive integer, and $a,a_j=-1,0,1,2$.

2. Introduction

The computational power of quantum computers has already been shown through several efficient quantum algorithms [1,2,3]. After Deutsch and Jozsa [1] designed the first quantum algorithm to demonstrate an advantage of quantum computers over classical computers, Shor [2] constructed quantum polynomial-time algorithms for the integer factoring problem and the discrete logarithm problem, and Grover [3] constructed a quantum algorithm that can find a particular item in $O(\sqrt{N})$ time when an unstructured list of N items are given. In order for these powerful algorithms to be successfully executed the purity of quantum states should be preserved during the process of computation. Unfortunately, quantum systems are always susceptible to the interaction with environments and so it is necessary to devise methods to correct operational errors and to control decoherence for reliable quantum computation and communication. The first effort toward this was made by Shor who showed that it is possible to correct errors by using a redundant quantum register and presented a nine-qubit code [4]. Since then many binary quantum error-correcting codes have been developed [5,6,7,8,9]. Calderbank and Shor [5], and Steane [6] invented an efficient procedure, so-called Calderbank-Shor-Steane (CSS) construction, of constructing binary quantum codes from special families of binary classical codes. In general, a quantum code can be represented by a common eigenspace of a set of linear operators acting on quantum systems and this representation is called a quantum stabilizer code [10]. Quantum stabilizer codes are closely related with classical self-orthogonal codes with respect to the symplectic inner product [11,12,13]. The necessary and sufficient condition to correct quantum errors was given by Knill and Laflamme [14] (see also [10,15]). Knill also provided a group representation of a non-binary unitary error basis [16,17]. The first non-binary code is a $[[5,1,3]]_q$ code for a positive integer q that was constructed by using the multiplicative group character [18,19]. It was also shown that quantum stabilizer codes over finite fields can be constructed from classical self-orthogonal codes with respect to the symplectic inner product [20,21]. Through the generalization of the binary CSS construction to finite fields quantum Reed-Solomon (RS) codes were obtained from classical RS codes [22,23]. Quantum twisted codes [24] and quantum Reed-Muller (RM) codes [25] were derived from classical twisted Bose-Chaudhuri-Hocquenghem (BCH) codes and classical RM codes, respectively.

For reliable transmission of quantum information, quantum codes need to be robust against operational errors and decoherence caused by environments. It is desirable to design error-correcting codes with as large distances as possible. It is because an error induces perturbation on the positions of codewords in a code space, and the farther the codewords, the more chance to correct the error. However, the distances of quantum error-correcting codes are bounded by the quantum Singleton bound [14,20]. To be more precise, an $[[n,k,d]]_q$ quantum error-correcting code with distance d that encodes k q-ary quantum systems into n q-ary quantum systems should satisfy $n-k \geq 2(d-1)$, which is a quantum analogue of the Singleton bound, $n-k \geq d-1$ for an $[n,k,d]_q$ classical error-correcting code which is a q-ary classical error-correcting code of length n, dimension k and distance d. A quantum error-correcting code that has the maximal distance saturating the quantum Singleton bound is called a quantum maximum distance separable (MDS) code and is most robust against errors for given n and k. Up to now several families of non-binary quantum MDS codes have been developed such as quantum twisted codes with parameters $[[p^{2m}+1, p^{2m}-3,3]]_{p^m}$ and $[[p^{2m}, p^{2m}-4,3]]_{p^m}$ [24], quantum RS codes with parameters $[[p^m-1,k,\frac{1}{2}(p^m-k+1)]]_{p^m}$ and $[[p^m,k,\frac{1}{2}(p^m-k+2)]]_{p^m}$ [23], quantum RM codes with parameters $[[(\nu+1)p^m,(\nu+1)(p^m-2),\nu+2]]_{p^m}$ for $0 \leq \nu \leq p^m-2$ [25], and quantum MDS codes with parameters $[[n,k,\frac{1}{2}(n-k+2)]]_{p^m}$ and $[[p^{2m}-s,k,\frac{1}{2}(p^{2m}-s-k+2)]]_{p^m}$ for all $3 \leq n \leq p^m$ and some s [26,27]. It is noted that all known quantum MDS codes were constructed over finite fields except a $[[5,1,3]]_q$ code.

Most of the previous non-binary quantum codes are based on finite fields. However, the dimensions of quantum systems to encode quantum information do not have to be a power of a prime. Thus it is necessary to consider quantum codes over alphabets of arbitrary size. To circumvent the difficulty in dealing with composite alphabets, we utilize an abelian group structure on alphabets instead of the conventional finite field structure. We label the basis states of a quantum system by elements in an abelian group and construct a unitary operator basis consisting of translation and phase-rotation operators, which can be seen as a natural generalization of the Pauli spin operators acting on qubits. Using the group structure of alphabets we exploit quantum stabilizer codes over quantum systems of which dimensions are composite numbers and show that quantum stabilizer codes over composite alphabets are related to classical self-orthogonal codes with respect to the symplectic inner product. We also develop CSS construction over composite alphabets. The CSS construction gives a systematic way to construct quantum codes from classical ones. We also construct the direct sum of error-correcting codes, which we call a coadunate code, to give rise to a error-correcting code with a new parameter, which plays an essential role in constructing error-correcting codes over composite alphabets from error-correcting codes over finite fields. Actually, error-correcting codes with the same length can be joined to comprise an error-correcting code over the direct sum of the alphabets, which is accomplished by conjoining heterogeneous codewords by components. The generalized CSS construction and the coadunate method can be used to construct quantum MDS codes over composite alphabets. Indeed, we obtain $[n=p_j^{m_j}+a_j,k,n-k+1]_{\prod p_j^{m_j}}$ classical coadunate RS (and MDS) codes and $[[n=p_j^{m_j}+a_j,k,\frac{1}{2}(n-k+2)]]_{\prod p_j^{m_j}}$ quantum coadunate RS (and MDS) codes over $\sum GF(p_j{}^{m_j})$, including families of $[[p^m+1,k,\frac{1}{2}(p^m-k+3)]]_{p^m}$ doubly-extended RS codes and

$[[2^m+2, k, \frac{1}{2}(2^m-k+4)]]_{2^m}$ triply-extended RS codes where p and p_j are primes and $a_j = -1,0,1,2$. We also construct $[[n=(\nu+1)p_1^{m_1} = p_2^{m_2}+a, k, \frac{1}{2}(n-k+2)]]_{p_1^{m_1}p_2^{m_2}}$ quantum coadunate MDS codes by conjoining quantum RS codes and quantum RM codes where $0 \le \nu \le p_1^{m_1}-2$ and $a = -1,0,1,2$. Moreover, when p is a prime and q is a positive integer we construct quantum MDS codes with parameters $[[n, n-2, 2]]_{2^m}$, $[[6,0,4]]_{2^m}$, $[[p^{2c}-s, k, \frac{1}{2}(p^{2c}-s-k+2)]]_{p^m}$ for some $-1 \le s \le p^{2c}$ and $c \mid m$, $[[p^{2m/3}-s, k, \frac{1}{2}(p^{2m/3}-s-k+2)]]_{p^m}$ for some $-1 \le s \le p^{2m/3}$, $[[p^c+a, k, \frac{1}{2}(p^c+a-k+2)]]_{p^m}$ for some $c \le m$ and $a = -1,0,1,2$, and so forth.

3. Objectives

(1) **Construction of quantum error-correcting codes over alphabets of arbitrary size**
Building unitary operator bases for the set of linear operators acting on quantum systems of arbitrary dimension, we generalize the structure of stabilizer codes and develop the Calderbank-Shor-Steane (CSS) construction.

(2) **Invention of classical and quantum coadunate error-correcting codes**
Conjoining error-correcting codes over Galois fields, we construct classical and quantum coadunate codes over composite alphabets.

(3) **Construction of quantum maximum distance separable (MDS) codes**
Using the CSS construction and the direct sum method, we construct new families of quantum MDS codes over composite alphabets.

4. Research Accomplishments

The original goals were

(1) Finding non-binary error bases for quantum systems of prime-power dimension,
(2) Development of the CSS construction over Galois fields of odd characteristics,
(3) Extension of a hierarchical structure of classical MDS codes, and
(4) Construction of quantum MDS codes based on Reed-Solomon codes.

Fist of all, we accomplished all the original goals and took a step forward. We removed the restriction on the number of alphabets, which are used in labeling the basis of quantum systems, and contrived coadunate codes, which is useful in the construction of quantum MDS codes over composite alphabets. Furthermore, we attained many new families of classical and quantum (MDS) codes as well as the aimed codes.

Our research accomplishments are summarized as follows:

(1) We built a unitary operator basis for the set of linear operators acting on quantum systems of which dimensions are composite numbers.
(2) We generalized quantum stabilizer codes over alphabets of arbitrary size.

(3) We developed the CSS construction over composite alphabets to give a systematic way to construct quantum error-correcting codes from classical error-correcting codes.
(4) We contrived classical and quantum coadunate codes over composite alphabets by conjoining error-correcting codes over finite fields.
(5) We constructed infinitely many quantum MDS codes using our CSS construction and coadunate method.

5. Significance of Findings to the Field

(1) Removal of the restriction on the number of alphabets
(2) Analysis of coadunate MDS codes
(3) New families of classical and quantum MDS codes over composite alphabets

6. Application Areas

(1) Realization of quantum computers
A practical prototype of quantum computers has not yet been established, and the dimension of physical systems comprising a quantum register is still undetermined and may not be a power of a prime. On this account it is necessary to contrive a method constructing general quantum error-correcting codes over composite alphabets.
(2) Reliable quantum information processing
In order for quantum information to be kept pure or to be transmitted reliably through noisy channels, quantum error-correcting codes are required to have as large distances as possible. Because Quantum MDS codes have maximal distances, they are most suited for this purpose and are practically important. Our approach comprehends most of the previous methods based on Galois fields and gives broad families of quantum MDS codes.
(3) Quantum cryptography, especially quantum secret sharing
Quantum error-correcting codes are closely related with quantum secret sharing protocols and can be used in cryptographic schemes to share secret quantum information.

7. Personnel Supported

In addition to PI and CoPI, 5 graduate students have been supported.

8. Publication

(1) J. Kim, J. Choi, and D. P. Chi, “Quantum maximum distance separable codes over alphabets of arbitrary size,” a preprint, 2005; to be presented at ERATO conference on quantum information science, Tokyo, Japan, Aug. 26-30, 2005.

9. Participation at Conferences

(1) 8th Workshop on Quantum Information Processing, MIT, Boston, MA, USA, Jan. 13~17, 2005.

(2) Workshop on Quantum Information, Computation and Communication, IIT Kharagpur, Kharagpur, India, Feb. 15~18, 2005.

10. New Discoveries

(1) Representation and construction of quantum error-correcting codes over composite alphabets.
(2) New families of quantum MDS codes over composite alphabets.

11. Honers / Awards

None

12. Archival Documentation

Please refer to the attached paper.

13. Software / Hardware

None

14. References

[1] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proc. Roy. Soc. London Ser. A **400** (1985), 96-117; Deutsch and R. Jozsa, *Rapid solution of problems by quantum computation*, Proc. R. Soc. London, Ser. A **439** (1992), 553-558.

[2] P. W. Shor, *Algorithms for quantum computation: Discrete log and factoring*, In Proceedings of the 35th IEEE Symposium on Foundations of Computer Science, p.20-22, 1994.

[3] L. K. Grover, *Quantum mechanics helps in searching for a needle in a haystack*, Phys. Rev. Letts. **79** (1997), 325-328.

[4] P. W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A **52** (1995), 2493-2496.

[5] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exits*, Phys. Rev. A **54** (1996), 1098-1105.

[6] A. M. Steane, *Multiparticle interference and quantum error correction*, Proc. Roy. Soc. Lond. A **452** (1996), 2551-2577.

[7] M. Steane, *Quantum Reed-Muller Codes*, IEEE Trans. Information Theory **45** (1999), 1701-1703.

[8] E. Knill and R. Laflamme, *Concatenated quantum codes*, Los Alamos e-print archive, quant-ph/9608012 (1996).

[9] M. Grassl and T. Beth, *Cyclic quantum error-correcting codes and quantum shift registers*, Los Alamos e-print archive, quant-ph/9910061 (1999).

[10] D. Gottesmann, *Stabilizer codes and quantum error correction*, Los Alamos e-print archive, quant-ph/9705052 (1997).
[11] R. Cleve, *Quantum Stabilizer codes and classical linear codes*, Phys. Rev. A **55** (1997), 4054-4059.
[12] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum error correction and orthogonal geometry*, Phys. Rev. Lett. **78** (1997), 405-408.
[13] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum error correction via codes over GF(4)*, IEEE Trans. Information Theory **44** (1998),1369-1387.
[14] E. Knill and R. Laflamme, *A theory of quantum error-correcting codes*, Phys. Rev. A **55** (1997), 900-911.
[15] D. Gottesmann, *An introduction to quantum error correction*, Los Alamos e-print archive, quant-ph/0004072 (2000).
[16] E. Knill, *Non-binary unitary error bases and quantum codes*, Los Alamos e-print archive, quant-ph/9608048 (1996).
[17] E. Knill, *Group representations, error bases and quantum codes*, Los Alamos e-print archive, quant-ph/9608049 (1996).
[18] H. F. Chau, *Correcting quantum errors in higher spin system*, Phys. Rev. A **55** (1997), R839-R841.
[19] H. F. Chau, *Five quantum register error correction code for higher spin system*, Phys. Rev. A **56** (1997), R1-R4.
[20] E. M. Rains, *Nonbinary quantum codes*, IEEE Trans. on Information Theory **45** (1999), 1827-1832.
[21] A. Ashikhmin and E. Knill, *Nonbinary stabilizer codes*, Los Alamos e-print archive, quant-ph/0005008 (2000).
[22] M. Grassl, W. Geiselmann and T. Beth, *Quantum Reed Solomon codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-13), Lecture Notes in Computer Science, Vol. 1719, Springer-Verlag, p.231-244, 1999.
[23] D. P. Chi, J. Kim, J. Lee and S. Lee, *Quantum MDS codes*, KIAS Workshop on Quantum Computation and Quantum Information, Seoul, Korea, 2001.
[24] J. Bierbrauer and Y. Edel, *Quantum twisted codes*, Journal of Combinatorial Designs **8** (2000), 174-188.
[25] P. K. Sarvepalli and A. Klappenecker, *Nonbinary quantum Reed-Muller codes*, Los Alamos e-print archive, quant-ph/0502001 (2005).
[26] M. Grassl and T. Beth, *On optimal quantum codes*, Los Alamos e-print archive, quant-ph/0312164 (2003).
[27] M. Rötteler, M. Grassl, and T. Beth, *On quantum MDS codes*, Proceedings. International Symposium on Information Theory, p.356-356, 2004.

REPORT OF INVENTIONS AND SUBCONTRACTS

(Pursuant to "Patent Rights" Contract Clause) (See Instructions on back)

Form Approved
OMB No. 9000-0095
Expires Oct 31, 2004

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (9000-0095), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THIS ADDRESS. RETURN COMPLETED FORM TO THE CONTRACTING OFFICER.

1.a. NAME OF CONTRACTOR/SUBCONTRACTOR	c. CONTRACT NUMBER	2.a. NAME OF GOVERNMENT PRIME CONTRACTOR	c. CONTRACT NUMBER	3. TYPE OF REPORT *(X one)*
N/A	N/A	N/A	N/A	☐ a. INTERIM ☐ b. FINAL

b. ADDRESS *(Include ZIP Code)*	d. AWARD DATE *(YYYYMMDD)*	b. ADDRESS *(Include ZIP Code)*	d. AWARD DATE *(YYYYMMDD)*	4. REPORTING PERIOD *(YYYYMMDD)*
N/A	N/A	N/A	N/A	a. FROM b. TO

SECTION I - SUBJECT INVENTIONS

5. "SUBJECT INVENTIONS" REQUIRED TO BE REPORTED BY CONTRACTOR/SUBCONTRACTOR *(If "None," so state)*

NAME(S) OF INVENTOR(S) *(Last, First, Middle Initial)* a.	TITLE OF INVENTION(S) b.	DISCLOSURE NUMBER, PATENT APPLICATION SERIAL NUMBER OR PATENT NUMBER c.	ELECTION TO FILE PATENT APPLICATIONS *(X)* d.				CONFIRMATORY INSTRUMENT OR ASSIGNMENT FORWARDED TO CONTRACTING OFFICER *(X)* e.	
			(1) UNITED STATES		(2) FOREIGN			
			(a) YES	(b) NO	(a) YES	(b) NO	(a) YES	(b) NO
N/A	N/A	N/A	☐	☐	☐	☐	☐	☐

f. EMPLOYER OF INVENTOR(S) NOT EMPLOYED BY CONTRACTOR/SUBCONTRACTOR		g. ELECTED FOREIGN COUNTRIES IN WHICH A PATENT APPLICATION WILL BE FILED	
(1) (a) NAME OF INVENTOR *(Last, First, Middle Initial)*	(2) (a) NAME OF INVENTOR *(Last, First, Middle Initial)*	(1) TITLE OF INVENTION	(2) FOREIGN COUNTRIES OF PATENT APPLICATION
N/A	N/A	N/A	N/A
(b) NAME OF EMPLOYER	(b) NAME OF EMPLOYER		
N/A	N/A		
(c) ADDRESS OF EMPLOYER *(Include ZIP Code)*	(c) ADDRESS OF EMPLOYER *(Include ZIP Code)*		
N/A	N/A		

SECTION II - SUBCONTRACTS *(Containing a "Patent Rights" clause)*

6. SUBCONTRACTS AWARDED BY CONTRACTOR/SUBCONTRACTOR *(If "None," so state)*

NAME OF SUBCONTRACTOR(S) a.	ADDRESS *(Include ZIP Code)* b.	SUBCONTRACT NUMBER(S) c.	FAR "PATENT RIGHTS" d.		DESCRIPTION OF WORK TO BE PERFORMED UNDER SUBCONTRACT(S) e.	SUBCONTRACT DATES *(YYYYMMDD)* f.	
			(1) CLAUSE NUMBER	(2) DATE *(YYYYMM)*		(1) AWARD	(2) ESTIMATED COMPLETION
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

SECTION III - CERTIFICATION

7. CERTIFICATION OF REPORT BY CONTRACTOR/SUBCONTRACTOR *(Not required if: (X as appropriate))* ☐ **SMALL BUSINESS or** ☐ **NONPROFIT ORGANIZATION**

I certify that the reporting party has procedures for prompt identification and timely disclosure of "Subject Inventions," that such procedures have been followed and that all "Subject Inventions" have been reported.

a. NAME OF AUTHORIZED CONTRACTOR/SUBCONTRACTOR OFFICIAL *(Last, First, Middle Initial)*	b. TITLE	c. SIGNATURE	d. DATE SIGNED
Jinsoo Kim	Professor		June 23, 2005

DD FORM 882, DEC 2001 PREVIOUS EDITION IS OBSOLETE.

Reset

DD FORM 882 INSTRUCTIONS

GENERAL

This form is for use in submitting INTERIM and FINAL invention reports to the Contracting Officer and for use in reporting the award of subcontracts containing a "Patent Rights" clause. If the form does not afford sufficient space, multiple forms may be used or plain sheets of paper with proper identification of information by item number may be attached.

An INTERIM report is due at least every 12 months from the date of contract award and shall include (a) a listing of "Subject Inventions" during the reporting period, (b) a certification of compliance with required invention identification and disclosure procedures together with a certification of reporting of all "Subject Inventions," and (c) any required information not previously reported on subcontracts containing a "Patent Rights" clause.

A FINAL report is due within 6 months if contractor is a small business firm or domestic nonprofit organization and within 3 months for all others after completion of the contract work and shall include (a) a listing of all "Subject Inventions" required by the contract to be reported, and (b) any required information not previously reported on subcontracts awarded during the course of or under the contract and containing a "Patent Rights" clause.

While the form may be used for simultaneously reporting inventions and subcontracts, it may also be used for reporting, promptly after award, subcontracts containing a "Patent Rights" clause.

Dates shall be entered where indicated in certain items on this form and shall be entered in six or eight digit numbers in the order of year and month (YYYYMM) or year, month and day (YYYYMMDD). Example: April 1999 should be entered as 199904 and April 15, 1999 should be entered as 19990415.

1.a. Self-explanatory.

1.b. Self-explanatory.

1.c. If "same" as Item 2.c., so state.

1.d. Self-explanatory.

2.a. If "same" as Item 1.a., so state.

2.b. Self-explanatory.

2.c. Procurement Instrument Identification (PII) number of contract (DFARS 204.7003).

2.d. through 5.e. Self-explanatory.

5.f. The name and address of the employer of each inventor not employed by the contractor or subcontractor is needed because the Government's rights in a reported invention may not be determined solely by the terms of the "Patent Rights" clause in the contract.

Example 1: If an invention is made by a Government employee assigned to work with a contractor, the Government rights in such an invention will be determined under Executive Order 10096.

Example 2: If an invention is made under a contract by joint inventors and one of the inventors is a Government employee, the Government's rights in such an inventor's interest in the invention will also be determined under Executive Order 10096, except where the contractor is a small business or nonprofit organization, in which case the provisions of 35 U.S.C. 202(e) will apply.

5.g.(1) Self-explanatory.

5.g.(2) Self-explanatory with the exception that the contractor or subcontractor shall indicate, if known at the time of this report, whether applications will be filed under either the Patent Cooperation Treaty (PCT) or the European Patent Convention (EPC). If such is known, the letters PCT or EPC shall be entered after each listed country.

6.a. Self-explanatory.

6.b. Self-explanatory.

6.c. Self-explanatory.

6.d. Patent Rights Clauses are located in FAR 52.227.

6.e. Self-explanatory.

6.f. Self-explanatory.

7. Certification not required by small business firms and domestic nonprofit organizations.

7.a. through 7.d. Self-explanatory.

Quantum Maximum Distance Separable Codes over Alphabets of Arbitrary Size*

Jinsoo Kim[1] † Jeongwoon Choi[2] ‡ Dong Pyo Chi[2] §

[1] *School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea.*
[2] *School of Mathematical Science, Seoul National University, Seoul 151-742, Korea.*

Abstract. We consider quantum error-correcting codes over alphabets of arbitrary sizes. Using the structure of commutative rings on alphabets we generalize quantum stabilizer codes and extend the Calderbank-Shor-Steane construction over quantum systems of composite dimensions. We also present a method conjoining error-correcting codes into a maximum distance separable code.

Keywords: Quantum stabilizer codes, CSS construction, quantum maximum distance separable codes

1 Introduction

Codes meeting the Singleton bound with equality are traditionally called maximum distance separable (MDS) codes [1] and similarly quantum codes saturating the quantum Singleton bound [2, 3] are called quantum maximum distance separable (QMDS) codes. A series of work to construct QMDS codes has been performed [4, 5, 3, 6, 7, 8, 9] and most of them are constructed over finite fields. We consider QMDS codes over alphabets of arbitrary sizes. To compose an error basis over a composite alphabet, we endow an alphabet with the structure of a commutative ring and generalize quantum stabilizer and Calderbank-Shor-Steane (CSS) codes. We present a method to combine QMDS codes over Galois fields into a QMDS code over a composite alphabet.

2 Quantum Codes over Composite Alphabets

To label the basis states of q-dimensional quantum system $\mathcal{H}$, we use an alphabet $\mathcal{A} = \oplus_{j=1}^{l}\mathcal{A}_j$ with $\mathcal{A}_j = \mathbb{Z}_{p_j}^{m_j}$ and $q = p_1^{m_1}p_2^{m_2}\cdots p_l^{m_l}$, where p_j's are distinct primes for $j = 1, 2, \ldots, l$. Let $\alpha = (\alpha_{ijk}) \in \mathcal{A}^n$ be composed of an element $\alpha_{ijk} \in \mathbb{Z}_{p_j}$ where the indices i, j, and k represent the i-th component of $\mathcal{A}^n$, j-th component of $\mathcal{A} = \oplus_{j=1}^{l}\mathcal{A}_j$, and the k-th component of $\mathcal{A}_j = \mathbb{Z}_{p_j}^{m_j}$, respectively, for $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, l$, and $k = 1, 2, \ldots, m_j$. We define unitary operators U_α and V_β by $U_\alpha|\chi\rangle = |\chi - \alpha\rangle$ and $V_\beta|\chi\rangle = \langle\langle\beta, \chi\rangle\rangle|\chi\rangle$ for $\alpha, \beta, \chi \in \mathcal{A}^n$, where $\langle\langle\alpha, \beta\rangle\rangle = \prod_{j=1}^{l}\omega_{p_j}^{\langle\alpha_{(j)}, \beta_{(j)}\rangle}$ and $\langle\alpha_{(j)}, \beta_{(j)}\rangle = \sum_{i=1}^{n}\sum_{k=1}^{m_j}\alpha_{ijk}\beta_{ijk}$. Then $\mathcal{B} = \{E_{\alpha,\beta} = U_\alpha V_\beta : \alpha, \beta \in \mathcal{A}^n\}$ forms a unitary basis for the set of linear operators acting on $\mathcal{H}^n$, which can be seen as an extension of a unitary basis in [10]. We note that $E_{\alpha,\beta}E_{\gamma,\delta} = \overline{\langle\langle\beta, \gamma\rangle\rangle}E_{\alpha+\gamma,\beta+\delta}$ and $E_{\alpha,\beta}E_{\gamma,\delta} = \langle\langle\alpha, \delta\rangle\rangle\overline{\langle\langle\beta, \gamma\rangle\rangle}E_{\gamma,\delta}E_{\alpha,\beta}$. Thus $E_{\alpha,\beta}$ and $E_{\gamma,\delta}$ commute if and only if $\langle\langle\alpha, \delta\rangle\rangle\overline{\langle\langle\beta, \gamma\rangle\rangle} = 1$. Due to the Chinese remainder theorem, we have one more equivalent condition that $\langle\alpha_{(j)}, \delta_{(j)}\rangle - \langle\beta_{(j)}, \gamma_{(j)}\rangle \equiv 0 \pmod{p_j}$ for all j. When a classical code in $\mathcal{A}^n \oplus \mathcal{A}^n = (\mathcal{A} \oplus \mathcal{A})^n$ satisfies this condition, we say that it is self-orthogonal with respect to the symplectic inner product, where the symplectic inner product on $\mathcal{A} \oplus \mathcal{A}$ is defined by $\langle\langle\alpha, \delta\rangle\rangle\overline{\langle\langle\beta, \gamma\rangle\rangle}$ for $(\alpha, \beta), (\gamma, \delta) \in \mathcal{A} \oplus \mathcal{A}$. As usual, we can relate an element (α, β) of C to an element $E_{\alpha,\beta}$ of a stabilizer group $\mathcal{S}$.

Theorem 1 *(Stabilizer Codes) There exists a classical code C over $\mathcal{A} \oplus \mathcal{A}$ which is self-orthogonal with respect to the symplectic inner product if and only if there exists a quantum stabilizer code $\mathcal{H}_\mathcal{S}$ over $\mathcal{A}$.*

It is also possible to construct CSS codes over $\mathcal{A}$ in a similar way to those over finite fields in [11, 12, 13, 7].

Theorem 2 *(CSS Construction) Let C_1 be a classical code with parameter $[n, k_1, d_1]_q$ and C_2 be a subcode of C_1 with parameter $[n, k_2, d_2]_q$. Let $\mathcal{C}$ be the subspace of $\mathcal{H}^n$ spanned by the orthonormal set*

$$\left\{|\bar{w}\rangle = \frac{1}{\sqrt{q^{k_2}}}\sum_{v\in C_2}|v + w\rangle : \bar{w} \in C_1/C_2\right\}.$$

Then $\mathcal{C}$ is an $[[n, k_1 - k_2, d = \min\{d_1, d_2^\perp\}]]_q$ quantum code, where $d_2^\perp$ is the distance of the dual code $C_2^\perp$ of C_2 and $C_2^\perp = \{\alpha \in \mathcal{A}^n : \langle\alpha_{(j)}, \beta_{(j)}\rangle \equiv 0 \pmod{p_j}$ for all $\beta \in C_2$ and all $j\}$.

By Theorem 2 we can generate a QMDS code from two MDS codes C_1 and C_2 such that $k_1 + k_2 = n$. Indeed, we obtain $[[p^m + 1, k, (p^m - k + 3)/2]]_{p^m}$ and $[[2^m + 2, 2^m - 4, 4]]_{2^m}$ QMDS codes from doubly-extended and triply-extended Reed-Solomon (RS) codes, respectively. Moreover, an $[[n = p_j^{m_j} + a_j, k, (n - k + 2)/2]]_{\prod_{j=1}^{l} p_j^{m_j}}$ QMDS code comes from RS codes over composite alphabets.

3 QMDS Codes

We can construct a quantum code over a composite alphabet by conjoining quantum codes with the same length, regardless of their dimensions and distances. The following lemma is an extension of the method in [3].

*ERATO Conference on Quantum Information Science, 2005

† jkim@ee.snu.ac.kr
‡ cju@snu.ac.kr
§ dpchi@math.snu.ac.kr

Lemma 3 *(Coadunate Quantum Codes) If there exist* $((n, K_j, d_j))_{q_j}$ *codes for* $j = 1, 2, \ldots, l$, *then there also exists an* $((n, \prod_{j=1}^{l} K_j, d))_{\prod_{j=1}^{l} q_j}$ *code where* $d = \min\{d_1, d_2, \ldots, d_l\}$.

This construction is also applicable to classical codes similarly. Using Lemma 3 we can derive a necessary and sufficient condition for a quantum coadunate code to be QMDS.

Theorem 4 *(Coadunate QMDS Codes) Suppose that an* $((n, \prod_{j=1}^{l} K_j, d))_{\prod_{j=1}^{l} q_j}$ *code* $\mathcal{C}$ *is constructed by* $((n, K_j, d_j))_{q_j}$ *codes* $\mathcal{C}_j$ *over* $\mathcal{A}_j$ *for* $j = 1, 2, \ldots, l$. $\mathcal{C}$ *is QMDS if and only if* $\mathcal{C}_j$*'s are all QMDS and satisfy that* $K_1 = K_2 = \cdots = K_l$ *and* $d_1 = d_2 = \cdots = d_l$.

Some examples of coadunate QMDS codes constructed by Theorem 4 are listed in Table 1. QMDS codes with parameters (B), (C), (D) and (E) are constructed by merging quantum codes in [4, 6, 8, 9] with themselves, respectively, and QMDS codes with the rest parameters are the conjunctions of heterogeneous QMDS codes which are quantum RS codes or QMDS codes in [4, 6, 8, 9].

Quantum puncturing [3] and shortening [14] over finite fields, which can be generalized over composite alphabets, give QMDS codes with shortened lengths, which, however, are not always guaranteed. The conjoining method can be another complementary solution to construct QMDS codes with shortened lengths.

Table 1: Some Examples of Parameters in New QMDS Codes

Index	Parameter
(A)	$[[p^m + 1, k, (p^m + 3 - k)/2]]_{p^m}$ and $[[2^m + 2, 2^m - 4, 4]]_{2^m}$
(B)	$[[n, n, 1]]_{2^m}$ for $n \geq 1$, $[[n, n-2, 2]]_{2^m}$ for even n, and $[[6, 0, 4]]_{2^m}$
(C)	$[[p^{2c} + a, p^{2c} + a - 4, 3]]_{p^m}$ for $a = 0, 1$ and $c \mid m$
(D)	$[[p^{2c} - s, p^{2c} - s - 2d + 2, d]]_{p^m}$ for some s ,$1 \leq d \leq p^c$ and $c \mid m$
(E)	$[[p^{2c}, p^{2c} - 2\nu - 2, \nu + 2]]_{p^m}$ and $[[(\nu+1)p^c, (\nu+1)p^c - 2\nu - 2, \nu + 2]]_{p^m}$ for $0 \leq \nu \leq p^c - 2$ and $c \mid m$
(F)	$[[p^{(m+c)/2}, p^{(m+c)/2} - 2p^c, p^c + 1]]_{p^m}$ for $0 \leq c \leq m/3$
(G)	$[[p^{2m/3}, p^{2m/3} - 4, 3]]_{p^m}$
(H)	$[[p^{2m/3} + 1, p^{2m/3} - 3, 3]]_{p^m}$
(I)	$[[p^{2m/3} - s, k, (p^{2m/3} - s - k + 2)/2]]_{p^m}$ for some $s \geq 0$ and $[[p^c + a, k, (p^c + a - k + 2)/2]]_{p^m}$ for $2c \leq m$ and $a = -1, 0, 1, 2$
(J)	$[[n = p_1^{2m_1} + 1 = (\nu+1)p_2^{m_2}, k, \frac{n-k+2}{2}]]_{p_1^{m_1} p_2^{m_2}}$ for $0 \leq \nu \leq p_2^{m_2} - 2$
(K)	$[[n = (\nu+1)p_1^{m_1} = p_2^{m_2} + a, k, \frac{n-k+2}{2}]]_{p_1^{m_1} p_2^{m_2}}$ for $0 \leq \nu \leq p_1^{m_1} - 2$ and $a = -1, 0, 1, 2$
(L)	$[[n = p_j^{m_j} + a_j, k, (n-k+2)/2]]_{\prod_{j=1}^{l} p_j^{m_j}}$ for $a_j = -1, 0, 1, 2$ and prime p_j

Acknowledgement

This work was supported by AFOSR/AOARD under grant FA5209-04-P-0228 (AOARD-044-010).

References

[1] F. J. Macwilliams and N. J. A. Sloane, *The theory of error correcting codes,* North-Holland, 1977.

[2] E. Knill and R. Laflamme, *A theory of quantum error-correcting codes*, Phys. Rev. A **55** (1997), 900–911.

[3] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, 1999.

[4] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[5] H. F. Chau. Five quantum register error correction code for higher spin system. *Phys. Rev. A*, 56:R1–R4, 1997.

[6] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Combin. Des.*, 8:174–188, 2000.

[7] D. P. Chi, J. Kim, J. Lee and S. Lee. QMDS Codes. manuscript, presented at *KIAS Workshop on Quantum Computation and Quantum Information*, Seoul, Korea, 2001.

[8] M. Rötteler, M. Grassl and T. Beth. On QMDS codes. In *Proc. of ISIT.*, pages 356–356, 2004; M. Grassl and T.Beth, On optimal quantum codes. quant-ph/0312164, 2003.

[9] P. K. Sarvepalli and A. Klappenecker. Nonbinary quantum Reed-Muller codes. quant-ph/0502001, 2005.

[10] A. Ashikhmin and E. Knill. Nonbinary stabilizer codes. quant-ph/0005008, 2000.

[11] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exits. *Phys. Rev. A*, 54:1098–1105, 1996.

[12] A. M. Steane. Multiparticle interference and quantum error correction. *Proc. Roy. Soc. Lond. A*, 452:2551–2577, 1996.

[13] D. Aharonov and M. Ben-or. Fault-tolerant quantum computation with constant error. In *Proc. of the 29th ACM STOC.*, pages 176–188, 1997; quant-ph/9611025, 1996.

[14] D. Gottesmann. Stabilizer codes and quantum error correction. quant-ph/9705052, 1997.

Quantum Maximum Distance Separable Codes over Alphabets of Arbitrary Size

Jinsoo Kim*, Jeongwoon Choi†, and Dong Pyo Chi†

Abstract

We consider quantum error-correcting codes over alphabets of arbitrary size. Using the structure of commutative rings on alphabets we generalize quantum stabilizer codes and extend the Calderbank-Shor-Steane construction over quantum systems of composite dimensions. We also present a method conjoining error-correcting codes into a maximum distance separable code. Moreover, we construct quantum maximum distance separable codes, for example, with parameters $[[p^m + a, k, (p^m + a - k + 2)/2]]_{p^m}$, $[[p^{2c} - s, k, (p^{2c} - s - k + 2)/2]]_{p^m}$ for some $-1 \leq s \leq p^{2c}$ and $c|m$, $[[p^{2m/3} - s, k, (p^{2m/3} - s - k + 2)/2]]_{p^m}$ for some $-1 \leq s \leq p^{2m/3}$, $[[p^c + a, k, (p^c + a - k + 2)/2]]_{p^m}$ for some $c \leq m$, $[[n = p_j^{m_j} + a_j, k, (n - k + 2)/2]]_{\prod_{j=1}^{l} p_j^{m_j}}$, and so forth, where p and p_j are primes and $-1 \leq a, a_j \leq 2$.

1 Introduction

Quantum systems are always susceptible to the interaction with surroundings and thus it is necessary to correct operational errors and to control decoherence caused by environments for reliable quantum computation and communication. The first effort toward this was made by Shor [1] who showed that it is possible to correct errors by using redundant quantum registers and presented a nine-qubit error-correcting code. Since then, many binary quantum error-correcting codes that can be constructed from classical error-correcting codes have been developed [2, 3, 4, 5, 6]. The necessary and sufficient condition for correcting quantum errors was set up by Knill and Laflamme [7] (see also [8, 9]). For reliable transmission of quantum information, quantum codes need to be robust against operational errors and decoherence caused by environments. It is desirable to design quantum error-correcting codes that have as large distance as possible. However, the distance is restricted by the quantum Singleton bound [7, 10]. A quantum code saturating this bound is called a quantum maximum distance separable (QMDS) code. Several QMDS codes have been developed so far [11, 12, 13, 14, 15, 16]. All binary QMDS codes have been discovered and they have parameters $[[n, n, 1]]_2$, $[[n, n-2, 2]]_2$, $[[5, 1, 3]]_2$, and $[[6, 0, 4]]_2$ [11].

*School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea. E-mail: jkim@ee.snu.ac.kr

†School of Mathematical Science, Seoul National University, Seoul 151-742, Korea.

Knill [17, 18] provided a group representation of a non-binary unitary operator basis for quantum errors. The first non-binary quantum codes are a $[[5,1,3]]_q$ code, which is QMDS, and a $[[9,1,3]]_q$ code for a positive integer q and they were constructed by using the multiplicative group character [19, 12]. In general, a quantum code can be represented by a common eigenspace of a set of linear operators acting on quantum systems and this representation is called a quantum stabilizer code [8]. Quantum stabilizer codes are closely related to classical self-orthogonal codes with respect to the symplectic inner product [20, 21, 11]. Quantum stabilizer codes over finite fields can also be constructed from classical self-orthogonal codes with respect to the symplectic inner product [10, 22]. Calderbank and Shor [2], and Steane [3] provided very efficient procedure, so-called Calderbank-Shor-Steane (CSS) construction, for the construction of binary quantum codes from special families of binary classical codes. Through the extension of the binary CSS construction to finite fields [23, 14], quantum Reed-Solomon (QRS) codes [24, 14] and quantum Reed-Muller (QRM) codes [16] were obtained from classical Reed-Solomon (RS) and Reed-Muller (RM) codes, respectively. QRS codes with parameters $[[p^m-1,k,(p^m-k+1)/2]]_{p^m}$ and $[[p^m,k,(p^m-k+2)/2]]_{p^m}$ are QMDS [14], and QRM codes with parameters $[[p^{2m},p^{2m}-2\nu+2,\nu+2]]_{p^m}$ and $[[(\nu+1)p^m,(\nu+1)p^m-2\nu-2,\nu+2]]_p^m$, which is obtained by puncturing for $0\le\nu\le p^m-2$, are QMDS [16]. In the symplectic geometry, quantum twisted codes were developed from twisted Bose-Chaudhuri-Hocquenghem (BCH) codes which are also known as RS subfield subcodes [13]. Quantum twisted codes with parameters $[[p^{2m}+1,p^{2m}-3,3]]_{p^m}$ and $[[p^{2m},p^{2m}-4,3]]_{p^m}$ are QMDS. QMDS codes with parameters $[[n,k,(n-k+2)/2]]_{p^m}$ and $[[p^{2m}-s,k,(p^{2m}-s-k+2)/2]]_{p^m}$ for some s were constructed by using the hermitian inner product [15].

In this paper, we consider error-correcting codes for quantum systems of composite dimension. We construct a unitary operator basis by using the structure of a commutative ring with identity, and generalize the quantum stabilizer construction and the CSS construction over alphabets of arbitrary size. As an example, we construct $[[p^m+1,k,(p^m+3-k)/2]]_{p^m}$ quantum doubly-extended RS codes and $[[2^m+2,2^m-4,4]]_{2^m}$ quantum triply-extended RS codes by the CSS construction from doubly-extended RS (DERS) and triply-extended RS (TERS) codes, respectively. We also introduce a method to comprise a quantum error-correcting code over the direct sum of alphabets by conjoining heterogeneous codewords by components, and present a necessary and sufficient condition for a quantum code thus constructed to be QMDS. Indeed, infinitely many families of QMDS codes can be generated by this method. For example, QMDS codes with parameters $[[n,n,1]]_{2^m}(n\ge 1)$, $[[n,n-2,2]]_{2^m}$ (n even ≥ 2), $[[5,1,3]]_{2^m}$, and $[[6,0,4]]_{2^m}$ are attained from binary QMDS codes. The conjunction of non-binary QMDS codes in [13, 14, 15, 16] produce QMDS codes with parameters $[[p^{2c}-s,k,(p^{2c}-s-k+2)/2]]_{p^m}$ and $[[(\nu+1)p^c,(\nu+1)p^c-2\nu-2,\nu+2]]_{p^m}$ for $-1\le s\le p^{2c}$, $0\le\nu\le p^c-2$, and $c|m$. We also obtain QMDS codes with parameters $[[p^{2m/3}-s,k,(p^{2m/3}-s-k+2)/2]]_{p^m}$ for some $-1\le s\le p^{2m/3}$, $[[p^c+a,p^c+a-2d+2,d]]_{p^m}$, $[[n=(\nu+1)p_1^{m_1}=p_2^{m_2}+a,k,(n-k+2)/2]]_{p_1^{m_1}p_2^{m_2}}$ for $0\le\nu\le p_1^{m_1}$, $[[n=p_j^{m_j}+a_j,k,(n+2-k)/2]]_{\prod_{j=1}^{l}p_j^{m_j}}$, and so on, where p and p_j are primes and $-1\le a,a_j\le 2$. Some more examples are listed in Table 2 of Section 3.1.

This paper is organized as follows. In Section 2 we compose an error basis over a commutative ring with identity and generalize quantum stabilizer codes and CSS codes. Section 3 is devoted to the construction of QMDS codes. We introduce a method to combine codes over Galois fields into a code over a composite alphabet and present a necessary and sufficient condition for the resulting code to be MDS. We also extend puncturing and shortening over composite alphabets. We conclude the paper in Section 4.

2 Non-binary Codes over Composite Alphabets

This section begins with the construction of a basis for linear operators acting on quantum systems of arbitrary dimensions. For this purpose we equip an alphabet with the structure of a commutative ring with identity. Based on the error basis we generalize quantum stabilizer codes and CSS construction over composite alphabets.

2.1 Error Basis

Classical and quantum error-correcting codes defined over finite fields have efficient encoding and decoding schemes due to rich field structure. Although codes over group or ring might be less efficient than those over finite fields [25], they are useful in dealing with q-ary quantum systems when q is not restricted to a power of a prime. In this section, we construct an operational error basis on q-ary quantum systems for any positive integer q. Pauli operators play a role of unitary operator basis for the set of linear operators acting on binary quantum systems. Using the group character, the operator basis was generalized over Galois field $\mathrm{GF}(p^m)$ by Ashikhmin and Knill [22]. Although there exists another operator basis over $\mathrm{GF}(p)$ provided by Rains [10], we generalize the Ashikhmin and Knill's method to construct an operator basis over composite alphabets by using a commutative ring with identity.

For a positive integer q we denote by $\mathcal{H}$ the q-dimensional complex Hilbert space describing a q-ary quantum system $\mathbb{C}^q$ with its orthonormal basis $\{|a\rangle\}$ of which index a is chosen from an alphabet $\mathcal{A}$ with q letters. To compose an error basis over $\mathcal{A}$, we endow $\mathcal{A}$ with the structure of a commutative ring with identity. We regard $\mathcal{A}$ as $\oplus_{j=1}^{l}\mathbb{Z}_{q_j} = \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \cdots \oplus \mathbb{Z}_{q_l}$ and identify $a \in \mathcal{A}$ with $(a_1, a_2, \ldots, a_l) \in \oplus_{j=1}^{l}\mathbb{Z}_{q_j}$ where $q = q_1 q_2 \cdots q_l$ and $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a ring of integers modulo n. Under this relation we will write $|a\rangle \equiv |a_1, a_2, \ldots, a_l\rangle = |a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_l\rangle$. We define a weighted inner product on $\mathcal{A}$ by $\langle a, b\rangle_q = \sum_{j=1}^{l} a_j b_j \hat{q}_j$ for $a, b \in \mathcal{A}$ where $\hat{q}_j = q/q_j$. To construct a basis for $\mathrm{End}(\mathcal{H})$ consisting of all endomorphisms on $\mathcal{H}$, we will make use of a symmetric bicharacter of $\mathcal{A}$ defined by

$$\omega_q^{\langle a,b\rangle_q} = \prod_{j=1}^{l} \omega_{q_j}^{a_j b_j} \tag{1}$$

for $a, b \in \mathcal{A}$ where $\omega_q = e^{2\pi\iota/q}$ and $\omega_{q_j} = e^{2\pi\iota/q_j}$ are primitive q and q_j-th roots of unity, respectively. Especially when $b = 1 = (1, 1, \ldots, 1)$, we will write $\omega_q^{\langle a\rangle_q} \equiv \omega_q^{\langle a,1\rangle_q} = \prod_{j=1}^{l} \omega_{q_j}^{a_j}$.

We define two kinds of unitary operators by

$$U_a|x\rangle = |x-a\rangle \qquad \text{and} \qquad V_b|x\rangle = \omega_q^{\langle b,x\rangle_q}|x\rangle \tag{2}$$

for $a, b, x \in \mathcal{A}$. We remark that this is a natural generalization of the Pauli spin operators σ_x and σ_z acting on binary quantum systems, and that when $\mathcal{A} = \mathbb{Z}_q$ these are merely $U_a = \sum_{x=0}^{q-1} |x-a\rangle\langle x|$ and $V_b = \sum_{x=0}^{q-1} \omega_q^{xb}|x\rangle\langle x|$. Since $U_aU_b = U_{a+b}$, $V_aV_b = V_{a+b}$, and $U_aV_b = \omega_q^{\langle a,b\rangle_q} V_bU_a$, we have

$$(U_aV_b)(U_cV_d) = \omega_q^{\langle a,d\rangle_q - \langle b,c\rangle_q}(U_cV_d)(U_aV_b)$$

and

$$\mathrm{tr}(U_aV_b) = \begin{cases} 0 & \text{for } (a,b) \neq (0,0), \\ q & \text{for } (a,b) = (0,0). \end{cases}$$

Hence the set $\{U_aV_b : a, b \in \mathcal{A}\}$ forms an orthogonal basis for $\mathrm{End}(\mathcal{H})$ under the trace inner product $\langle A, B\rangle = \mathrm{tr}(A^\dagger B)$ for $A, B \in \mathrm{End}(\mathcal{H})$. Especially when q is an odd prime, every nonidentity operator U_aV_b is of order q since $U_a^q = I$, $V_b^q = I$, and $(U_aV_b)^q = \omega_q^{-\langle a,b\rangle_q (q-1)q/2}(U_a)^q(V_b)^q = I$. To sum up, we have the following theorem.

Theorem 2.1. *The set $\mathcal{B} = \{U_aV_b : a, b \in \mathcal{A}\}$ consisting of q^2 unitary operators is an orthogonal basis for $\mathrm{End}(\mathcal{H})$ with respect to the trace inner product. If q is an odd prime number, then every nonidentity element of $\mathcal{B}$ has order q.*

Sometimes it is convenient to consider an alphabet as a direct sum of finite fields. We first consider the case when $q = p^m$ for a prime p. To represent symbols for an orthogonal basis for q-dimensional Hilbert space, we will identify $\mathcal{A}$ with a commutative ring $\mathbb{Z}_p^m = Z_p^{\oplus m}$ instead of a Galois field $\mathrm{GF}(p^m)$. Using the unitary operators in (2) we can obtain operators $U_aV_b = (U_{a_1}V_{b_1}) \otimes (U_{a_2}V_{b_2}) \otimes \cdots \otimes (U_{a_m}V_{b_m})$ for $a = (a_1, a_2, \ldots, a_m), b = (b_1, b_2, \ldots, b_m) \in \mathbb{Z}_p^m$. Then the set $\{U_aV_b : a, b \in \mathbb{Z}_p^m\}$ forms an orthogonal basis for $\mathrm{End}(\mathcal{H})$ by Theorem 2.1. This basis used to construct quantum error-correcting codes over finite fields in [22].

For a positive integer q we utilize its unique prime factorization $q = p_1^{m_1} \cdots p_l^{m_l}$ where p_j's are distinct prime numbers. To label basis states of $\mathcal{H}$, we use an alphabet $\mathcal{A} = \oplus_{j=1}^l \mathcal{A}_j$ where $\mathcal{A}_j = \mathbb{Z}_{p_j}^{m_j}$ for $j = 1, 2, \ldots, l$. Furthermore, we symbolize the basis states for a tensor product $\mathcal{H}^n = \mathcal{H}^{\otimes n}$ of $\mathcal{H}$ using the elements in $\mathcal{A}^n$. For $\mathbf{a} = (a_{ijk}) \in \mathcal{A}^n$, the element $a_{ijk} \in \mathbb{Z}_{p_j}$ is the i-th component of $\mathcal{A}^n$, j-th component of $\mathcal{A} = \oplus_{j=1}^l \mathcal{A}_j$, and the k-th component of $\mathcal{A}_j = \mathbb{Z}_{p_j}^{m_j}$ for $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, l$, and $k = 1, 2, \ldots, m_j$. For convenience' sake, we introduce notations $\mathbf{a}^{(i)} = (a_{ijk})_{j,k} \in \mathcal{A}$ and $\mathbf{a}_{(j)} = (a_{ijk})_{i,k} \in \mathcal{A}_j^n$. By (2) unitary operators on $\mathcal{H}^n$ can be constructed by

$$\begin{aligned} E_{\mathbf{a},\mathbf{b}} &= (U_{\mathbf{a}^{(1)}}V_{\mathbf{b}^{(1)}}) \otimes (U_{\mathbf{a}^{(2)}}V_{\mathbf{b}^{(2)}}) \otimes \cdots \otimes (U_{\mathbf{a}^{(n)}}V_{\mathbf{b}^{(n)}}) \\ &= (U_{\mathbf{a}_{(1)}}V_{\mathbf{b}_{(1)}}) \otimes (U_{\mathbf{a}_{(2)}}V_{\mathbf{b}_{(2)}}) \otimes \cdots \otimes (U_{\mathbf{a}_{(l)}}V_{\mathbf{b}_{(l)}}). \end{aligned}$$

Since $\mathrm{tr}(A \otimes B) = \mathrm{tr}A\,\mathrm{tr}B$, nonidentity operators $E_{\mathbf{a},\mathbf{b}}$ have trace zero and thus are orthogonal to each other under the trace inner product. Therefore we have the following theorem.

Corollary 2.1. *The set* $\mathcal{B} = \{E_{\mathbf{a},\mathbf{b}} : \mathbf{a}, \mathbf{b} \in \mathcal{A}^n\}$ *consisting of unitary operators is a basis for* $\mathrm{End}(\mathcal{H}^n)$.

We remark that the operator basis $\mathcal{B}$ over a commutative ring with identity is an extension of the operator basis over a finite field in [22].

2.2 Stabilizer Codes

Quantum stabilizer codes can be constructed over composite alphabets based on the basis $\mathcal{B}$ in Corollary 2.1 and they can be represented by classical self-orthogonal codes with respect to a weighted symplectic inner product.

The set $\mathcal{E} = \left\{\omega_q^{\langle a \rangle_q} E_{\mathbf{a},\mathbf{b}} : a \in \mathcal{A} \text{ and } \mathbf{a}, \mathbf{b} \in \mathcal{A}^n\right\}$ is a group of order $q^{2n} p_1 p_2 \cdots p_l$. Let $\mathcal{S}$ be an abelian subgroup of $\mathcal{E}$, and $\mathcal{H}_\mathcal{S}$ be a common eigenspace of all elements in $\mathcal{S}$ with eigenvalue 1, that is, $|\psi\rangle \in \mathcal{H}_\mathcal{S}$ if and only if $M|\psi\rangle = |\psi\rangle$ for all $M \in \mathcal{S}$. Then $\mathcal{H}_\mathcal{S}$ is called a quantum stabilizer code, and $\mathcal{S}$ is called a stabilizer group of $\mathcal{H}_\mathcal{S}$ because $\mathcal{S}$ preserves $\mathcal{H}_\mathcal{S}$. We remark that any other common eigenspaces are equivalent to $\mathcal{H}_\mathcal{S}$ and can also be used as quantum stabilizer codes because it is possible to construct the corresponding stabilizer groups by multiplying phase factors. A K-dimensional q-ary quantum error-correcting code of length n with distance d is denoted by $((n, K, d))_q$. A quantum code with distance d can detect $d-1$ errors and hence can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. We define the weight of $E_{\mathbf{a},\mathbf{b}}$ by the number of non-trivial $U_{\mathbf{a}^{(i)}} V_{\mathbf{b}^{(i)}}$'s in $E_{\mathbf{a},\mathbf{b}}$ and denote it by $\mathrm{wt}(E_{\mathbf{a},\mathbf{b}})$. In quantum stabilizer codes, the distance d becomes the minimum of $\{\mathrm{wt}(E_{\mathbf{a},\mathbf{b}}) : E_{\mathbf{a},\mathbf{b}} \in C(\mathcal{S}) \backslash \mathcal{S}\}$ where $C(\mathcal{S})$ is the centralizer of $\mathcal{S}$, because the operators in $C(\mathcal{S}) \backslash \mathcal{S}$ induce nontrivial automorphisms on $\mathcal{H}_\mathcal{S}$ and thus are non-detectable errors. The order of a stabilizer group $\mathcal{S}$ is the product of the orders of its generators and hence the dimension of $\mathcal{H}_\mathcal{S}$ equals $q^n/|\mathcal{S}|$ as in the case of quantum stabilizer codes over finite fields [22] where $|\mathcal{S}|$ is the number of elements of $\mathcal{S}$.

Theorem 2.2. *If a quantum stabilizer code* $\mathcal{H}_\mathcal{S}$ *has parameter* $((n, K, d))_q$, *then* $K = q^n/|\mathcal{S}|$.

The stabilizer group $\mathcal{S}$ is equivalent to a classical code. To see this, let us consider the quotient group $\bar{\mathcal{E}} = \mathcal{E}/\mathcal{Z}$ where $\mathcal{Z} = \left\{\omega_q^{\langle a \rangle_q} I^{\otimes n} : a \in \mathcal{A}\right\}$ is the center of $\mathcal{E}$ with $p_1 p_2 \cdots p_l$ elements. Then its representatives can be chosen from $\mathcal{B}$ and $\bar{\mathcal{E}} = \{E_{\mathbf{a},\mathbf{b}}\mathcal{Z} : E_{\mathbf{a},\mathbf{b}} \in \mathcal{B}\}$ is isomorphic to a group $V = \{(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathcal{A}^n\}$. The quotient subgroup $\bar{\mathcal{S}} = \mathcal{S}/\mathcal{Z}$ of $\bar{\mathcal{E}}$ is also a stabilizer group corresponding to the quantum stabilizer code equivalent to $\mathcal{H}_\mathcal{S}$, and $\bar{\mathcal{S}}$ is isomorphic to a subgroup C of V which can be regarded as a classical code. Hence we can identify an element $E_{\mathbf{a},\mathbf{b}}$ of $\bar{\mathcal{S}}$ with an element $(\mathbf{a}, \mathbf{b})$ of a classical code C over $\mathcal{A}$ and there is a one-to-one correspondence between a quantum stabilizer group and a classical code.

When $\mathcal{A}$ is a finite field and $q = p^m$, for $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{c}, \mathbf{d})$ in $\mathcal{A}^n \times \mathcal{A}^n = (\mathcal{A} \times \mathcal{A})^n$ an alternating bilinear form $\langle\langle(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d})\rangle\rangle \equiv \langle \mathbf{a}, \mathbf{d}\rangle - \langle \mathbf{b}, \mathbf{c}\rangle$ is called a symplectic inner product on $\mathcal{A}^n \times \mathcal{A}^n$ where $\langle \mathbf{a}, \mathbf{b}\rangle = \sum_{i=1}^{n} \sum_{j=1}^{l} \sum_{k=1}^{m_j} a_{ijk} b_{ijk}$ is the usual inner product on $\mathcal{A}^n$, and we say that a subgroup of V is self-orthogonal with respect to

the symplectic inner product if it satisfies $\langle\langle(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{d})\rangle\rangle \equiv 0 \pmod{p}$. C should be self-orthogonal with respect to the symplectic inner product by the commutativity of $\mathcal{S}$ [10, 22]. When $\mathcal{A}$ is a direct sum of finite fields we need a special form of a symplectic inner product. We note that operators in $\mathcal{E}$ satisfy

$$E_{\mathbf{a},\mathbf{b}}E_{\mathbf{c},\mathbf{d}} = \omega_q^{-\langle\mathbf{b},\mathbf{c}\rangle_q} E_{\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{d}},$$
$$E_{\mathbf{a},\mathbf{b}}E_{\mathbf{c},\mathbf{d}} = \omega_q^{\langle\mathbf{a},\mathbf{d}\rangle_q-\langle\mathbf{b},\mathbf{c}\rangle_q} E_{\mathbf{c},\mathbf{d}}E_{\mathbf{a},\mathbf{b}}.$$

So, multiplication in $\bar{\mathcal{S}}$ corresponds to addition in C and for this reason a quantum stabilizer code is also called a quantum additive code [11]. Moreover, $E_{\mathbf{a},\mathbf{b}}$ and $E_{\mathbf{c},\mathbf{d}}$ commute if and only if $\omega_q^{\langle\mathbf{a},\mathbf{d}\rangle_q-\langle\mathbf{b},\mathbf{c}\rangle_q} = 1$. For $(\mathbf{a},\mathbf{b})$ and $(\mathbf{c},\mathbf{d})$ in $\mathcal{A}^n \times \mathcal{A}^n = (\mathcal{A}\times\mathcal{A})^n$ we will define the weighted symplectic inner product $\langle\langle(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{d})\rangle\rangle_q$ by $\langle\mathbf{a},\mathbf{d}\rangle_q - \langle\mathbf{b},\mathbf{c}\rangle_q$ modified from a symplectic inner product for a finite field in [10, 22], and say that a classical code over $\mathcal{A}\times\mathcal{A}$ is self-orthogonal with respect to the weighted symplectic inner product if it satisfies that $\langle\langle(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{d})\rangle\rangle_q \equiv 0 \pmod{p_1p_2\cdots p_l}$. After all, we obtain the following result.

Theorem 2.3. *There exists a self-orthogonal code C in $\mathcal{A}^n \times \mathcal{A}^n$ with respect to the weighted symplectic inner product if and only if there exists a quantum stabilizer code $\mathcal{H}_{\mathcal{S}}$ over $\mathcal{A}$.*

Due to the fact that p_j's are all distinct prime, we have one more equivalent condition to self-orthogonality as shown in the following lemma which can be proved by the Chinese remainder theorem.

Lemma 2.1. $\omega_q^{\langle\langle(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{d})\rangle\rangle_q} = 1$ *if and only if* $\langle\langle(\mathbf{a}_{(j)},\mathbf{b}_{(j)}),(\mathbf{c}_{(j)},\mathbf{d}_{(j)})\rangle\rangle \equiv 0 \pmod{p_j}$ *for each j.*

Proof. Let us provide a proof through a direct calculation. We have $\omega_q^{\langle\langle(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{d})\rangle\rangle_q} = \omega_q^{\sum_{j=1}^{l}\langle\langle(\mathbf{a}_{(j)},\mathbf{b}_{(j)}),(\mathbf{c}_{(j)},\mathbf{d}_{(j)})\rangle\rangle\hat{p_j}} = \omega^{\sum_{j=1}^{l}\langle\langle(\mathbf{a}_{(j)},\mathbf{b}_{(j)}),(\mathbf{c}_{(j)},\mathbf{d}_{(j)})\rangle\rangle\hat{\hat{p}_j}}$ where $\omega = e^{2\pi\iota/(p_1p_2\cdots p_l)}$, $\hat{p_j} = q/p_j$ and $\hat{\hat{p}_j} = (p_1p_2\cdots p_l)/p_j$. Thus $\omega_q^{\langle\langle(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{d})\rangle\rangle_q} = 1$ if and only if $\sum_{j=1}^{l}\langle\langle(\mathbf{a}_{(j)},\mathbf{b}_{(j)}),(\mathbf{c}_{(j)},\mathbf{d}_{(j)})\rangle\rangle\hat{\hat{p}_j} \equiv 0 \pmod{p_1p_2\cdots p_l}$ if and only if $\langle\langle(\mathbf{a}_{(j)},\mathbf{b}_{(j)}),(\mathbf{c}_{(j)},\mathbf{d}_{(j)})\rangle\rangle \equiv 0 \pmod{p_j}$ for each j, because all terms except $\langle\langle(\mathbf{a}_{(j)},\mathbf{b}_{(j)}),(\mathbf{c}_{(j)},\mathbf{d}_{(j)})\rangle\rangle\hat{\hat{p}_j}$ have a divisor p_j. □

Suppose that $C_j = \{(\mathbf{a}_{(j)},\mathbf{b}_{(j)}) \in \mathcal{A}_j^n \times \mathcal{A}_j^n : (\mathbf{a},\mathbf{b}) \in C\}$. Then C_j is a self-orthogonal code with respect to the symplectic inner product by Lemma 2.1 and we obtain the following corollary.

Corollary 2.2. *There exists self-orthogonal codes C_j in $\mathcal{A}_j^n \times \mathcal{A}_j^n$ with respect to the symplectic inner product if and only if there exists a quantum stabilizer code $\mathcal{H}_{\mathcal{S}}$ over $\mathcal{A}$.*

Let $C^{\perp} = \{(\mathbf{a},\mathbf{b}) \in \mathcal{A}^n \times \mathcal{A}^n : \langle\langle(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{d})\rangle\rangle_q \equiv 0 \pmod{p_1p_2\cdots p_l}$ for all $(\mathbf{c},\mathbf{d}) \in C\}$ be the dual code of C with respect to the weighted symplectic inner product. Then, C and $C^{\perp}$ correspond to the stabilizer group $\mathcal{S}$ and its centralizer $C(\mathcal{S})$, respectively. Thus the minimum weight of the codewords in $C^{\perp} \setminus C$ is equal to the distance of the quantum stabilizer code.

2.3 CSS Codes

The CSS construction gives a way to construct a quantum code over a Galois field, which is called a CSS code, from a classical code and its subcode [2, 3, 23, 14]. We generalize the CSS construction over alphabets of arbitrary size by using the unitary operator basis $\mathcal{B}$ in Corollary 2.1. The generalization is straightforward and so we only sketch the procedure briefly. For classical codes C_1 and C_2 over $\mathcal{A}$ such that $C_2 \subset C_1$, the CSS construction over $\mathcal{A}$ encodes quantum information to pure quantum states with equally distributed phases such as $|\bar{w}\rangle = \frac{1}{\sqrt{q^{k_2}}} \sum_{v \in C_2} |v + w\rangle$ for $\bar{w} \in C_1/C_2$. Let us suppose that a quantum state $|\bar{w}\rangle$ is transformed into $U_{\mathbf{a}} V_{\mathbf{b}} |\bar{w}\rangle = \frac{1}{\sqrt{q^{k_2}}} \sum_{v \in C_2} \langle\langle \mathbf{b}, v+w \rangle\rangle |v + w - \mathbf{a}\rangle$ by an error $U_{\mathbf{a}} V_{\mathbf{b}} \in \mathcal{B}$. To correct the error caused by the translation operator, we prepare a unitary transformation $T : |\mathbf{a}\rangle_D \otimes |a\rangle_A \to |\mathbf{a}\rangle_D \otimes |H_1 \mathbf{a} + a\rangle_A$ where the subscripts D and A denote the quantum systems of the data register and the ancillary register, respectively, and H_1 is a parity check matrix of C_1. To correct errors caused by phase rotation operators, we shift phase errors to translation errors through the quantum Fourier transformation $\bigotimes_{j=1}^{l} \mathrm{QFT}_{p_j}^{n_{m_j}}$ and then perform a unitary transformation $T' : |\mathbf{a}\rangle_D \otimes |a\rangle_A \to |\mathbf{a}\rangle_D \otimes |G_2 \mathbf{a} + a\rangle_A$ where G_2 is a generator matrix of C_2. After all, we can correct translation errors and phase errors by using H_1 and G_2, respectively. Thus we obtain the following result.

Theorem 2.4. *(CSS Codes) Suppose that C_1 is a classical code with parameter $[n, k_1, d_1]_q$ and C_2 is a subcode of C_1 with parameter $[n, k_2, d_2]_q$. Let H_1 be an $(n - k_1) \times n$ parity check matrix of C_1 and G_2 be a $k_2 \times n$ generator matrix of C_2. Let $\mathcal{C}$ be the subspace of $\mathcal{H}^n$ spanned by an orthonormal set*

$$\left\{ |\bar{w}\rangle = \frac{1}{\sqrt{q^{k_2}}} \sum_{v \in C_2} |v + w\rangle : \bar{w} \in C_1/C_2 \right\}.$$

Then $\mathcal{C}$ is an $[[n, k_1 - k_2, d = \min\{d_1, d_2^{\perp}\}]]_q$ quantum code, where $d_2^{\perp}$ is the distance of the dual code $C_2^{\perp} = \{\mathbf{a} \in \mathcal{A}^n : \langle \mathbf{a}, \mathbf{b} \rangle_q \equiv 0 \pmod{p_1 p_2 \cdots p_l}$ for all $\mathbf{b} \in C_2\}$ of C_2.

In Theorem 2.4 the parameters $[n, k, d]_q$ and $[[n, k, d]]_q$ stand for a k-dimensional classical code and a q^k-dimensional quantum code, respectively, with length n and distance d. Theorem 2.4 will be used to generate quantum codes from classical codes over rings as well as over direct sums of finite fields in the subsequent section.

3 QMDS Codes

In this section, we present methods to construct quantum maximum distance separable codes based on quantum stabilizer codes and CSS codes over composite alphabets.

An $(n, K, d)_q$ code meeting the Singleton bound $d \leq n - \log_q K + 1$ with equality is called a maximum distance separable (MDS) code. It means that all of the possible codewords are as far away, algebraically, as possible in code space. A quantum analogue of the Singleton bound is $K \leq q^{n-2d+2}$ for an $((n, K, d))_q$ code and it is called the quantum Singleton bound [10]. In binary case, this can be simplified to

$n-k \geq 2(d-1)$ for an $[[n,k,d]]_2$ code [7]. A quantum code saturating the quantum Singleton bound is called a quantum maximum distance separable (QMDS) code.

Before going into QMDS codes over composite alphabets, we first consider classical MDS codes over composite alphabets which will be used to construct QMDS codes by the CSS construction later.

3.1 Classical Coadunate Codes

Error-correcting codes with the the same length over any alphabets can be conjoined to form a coadunate error-correcting code over the direct sum of their alphabets as shown in the following lemma.

Lemma 3.1. *(Coadunate Code) If there exist an $(n, K_j, d_j)_{q_j}$ code C_j over $\mathcal{A}_j$ for $j = 1, 2, \ldots, l$, then there exists an $(n, \prod_{j=1}^{l} K_j, d)_{\prod_{j=1}^{l} q_j}$ code C over $\prod_{j=1}^{l} \mathcal{A}_j$ where $d = \min\{d_1, d_2, \ldots, d_l\}$.*

Proof. We set $C = \{c = (a_1, a_2, \ldots, a_n) : a_i = (a_{i1}, a_{i2}, \ldots, a_{il}) \in \prod_{j=1}^{l} \mathcal{A}_j$ and $c_j = (a_{1j}, a_{2j}, \ldots, a_{nj}) \in C_j\}$. We show that the minimum weight of C is $d = \min\{d_1, d_2, \ldots, d_l\}$. Every codeword of C has weight greater than or equal to d, because for each j there exists a codeword $c_j \in C_j$ with $\mathrm{wt}(c_j) = d_j$. On the other hand, if $d = d_j$ then it is sufficient to find a codeword c of C with $\mathrm{wt}(c) = d_j$. If we set $c_i = (0, 0, \ldots, 0) \in C_i$ for all $i \neq j$ and $c_j \in C_j$ with $\mathrm{wt}(c_j) = d$, then the codeword c has weight d_j obviously. This completes the proof. □

For simplicity, we will call C constructed by Lemma 3.1 a coadunate code. Lemma 3.1 gives a way to construct an MDS code over a composite alphabet by merging classical MDS codes that have the same code length, dimension and distance.

Theorem 3.1. *(Coadunate MDS Code) Suppose that an $(n, \prod_{j=1}^{l} K_j, d)_{\prod_{j=1}^{l} q_j}$ code C is constructed by an $(n, K_j, d_j)_{q_j}$ code C_j over $\mathcal{A}_j$ for $j = 1, 2, \ldots, l$. If C is MDS, then every C_j is MDS and satisfies that $K_1 = K_2 = \cdots = K_l$ and $d_1 = d_2 = \cdots = d_l$ and vice versa.*

Proof. Suppose that C is MDS. By the Singleton bound $K_j \leq q_j^{n-d_j+1}$ for each C_j. Since $d = \min\{d_1, d_2, \ldots, d_l\}$, $K_j \leq q_j^{n-d_j+1} \leq q_j^{n-d+1}$ and thus $\prod_{j=1}^{l} K_j \leq \prod_{j=1}^{l} q_j^{n-d_j+1} \leq \prod_{j=1}^{l} q_j^{n-d+1}$. Therefore $K_j = q_j^{n-d_j+1} = q_j^{n-d+1}$ for all j, because C satisfies $\prod_{j=1}^{l} K_j = \prod_{j=1}^{l} q_j^{n-d+1}$. The converse is obvious (See, for example, [26]). □

There are infinitely many MDS codes satisfying the necessary conditions in Theorem 3.1. Especially, the following families of Reed-Solomon (RS) codes [27, 28] are easy to comply with these conditions: For a prime number p,

(i) $[p^m - 1, k, p^m - k]_{p^m}$ generalized RS (GRS) codes for $1 \leq k \leq p^m - 1$,

(ii) $[p^m, k, p^m - k + 1]_{p^m}$ extended RS (ERS) codes for $1 \leq k \leq p^m$,

(iii) $[p^m+1, k, p^m-k+2]_{p^m}$ doubly-extended RS (DERS) codes for some $1 \le k \le p^m+1$ [28], and

(iv) $[2^m+2, k, 2^m-k+3]_{2^m}$ triply-extended RS (TERS) codes for $k = 3,\ 2^m-1$.

From the families of RS codes over Galois fields in (i),(ii),(iii), and (iv), with the same length, dimension, and distance, regardless of their alphabets, we can construct MDS codes over the direct sum of Galois fields by Theorem 3.1. The following corollary shows an example of QMDS codes.

Corollary 3.1. *(Coadunate RS Codes) There exists an* $[n = p_j^{m_j} + a_j, k, n-k+1]_{\prod_{j=1}^{l} p_j^{m_j}}$ *code for* n *such that* $n = p_j^{m_j} + a_j$ *where* $a_j = -1, 0, 1, 2$ *and* p_j*'s are prime numbers.*

By Corollary 3.1, for example, we obtain a $[18 = 2^4+2 = 17+1, 3, 16]_{2^4 17}$ code over $\mathrm{GF}(2^4) \oplus \mathrm{GF}(17)$ from a $[18, 3, 16]_{2^4}$ TERS code and a $[18, 3, 16]_{17}$ DERS code. Similarly, a $[9 = 2^3+1 = 3^2, 2, 8]_{3^2 2^3}$ code over $\mathrm{GF}(3^2) \oplus \mathrm{GF}(2^3)$ is generated from a $[9, 2, 8]_{3^2}$ ERS code and a $[9, 2, 8]_{2^3}$ DERS code, and a $[26 = 3^3-1 = 5^2+1, 3, 24]_{3^3 5^2}$ code over $\mathrm{GF}(3^3) \oplus \mathrm{GF}(5^2)$ is constructed by conjoining a $[26, 3, 24]_{3^3}$ GRS code and a $[26, 3, 24]_{5^2}$ DERS code.

There are actually infinitely many families of RS codes satisfying the conditions in Theorem 3.1. In particular, let us consider a pair (p_1, p_2) of primes satisfying $n = p_1 + a_1 = p_2 + a_2$ for given n. When $a_1 - a_2 = \pm 2$, this pair of primes is called a twin prime and in this case there always exists an $[n = p_1+a_1 = p_2+a_2, k, n-k+1]_{p_1 p_2}$ code. There is a conjecture that there exist infinitely many twin primes, which has not yet been proved. However, it is widely believed that the conjecture is true [29].

3.2 CSS Construction over QMDS Codes

As shown in Theorem 2.4, the CSS construction is a method to construct quantum error-correcting codes from two classical codes, one of which is a subcode of the other. To construct QMDS codes through the CSS construction, we need more restriction on classical codes. The next theorem provides a sufficient condition for the CSS construction to give QMDS codes.

Theorem 3.2. *If there exist two MDS codes,* C_1 *with parameter* $[n, k_1, n-k_1+1]_q$ *and* C_2 *with parameter* $[n, k_2, n-k_2+1]_q$*, satisfying* $k_1 \ge k_2$*,* $k_1 + k_2 = n$*, and* $C_2 \subset C_1$*, then there exists a QMDS code* $\mathcal{C}$ *with parameter* $[[n, k_1-k_2, (n-k_1+k_2+2)/2]]_q$*.*

Proof. We note that $C_2^{\perp}$ is also MDS with parameter $[n, n-k_2, k_2+1]_q$. By Theorem 2.4, $\mathcal{C}$ has distance $d \ge \min\{n-k_1+1, k_2+1\}$ and hence we have $d \ge n-k_1+1$. On the other hand, by the quantum Singleton bound, the distance must satisfy $d \le n-k_1+1 = (n-k_1+k_2+2)/2$. Thus we obtain $d = n-k_1+1$ and so $\mathcal{C}$ is QMDS. □

When C is self-orthogonal, Theorem 3.2 with $C_1 = C^{\perp}$ and $C_2 = C$ gives the following result.

Corollary 3.2. *If there is an* $[n, k, n-k+1]_q$ *self-orthogonal and MDS code, then there exists an* $[[n, n-2k, k+1]]_q$ *QMDS code whenever* $1 \leq k \leq n/2$.

With the help of Theorem 3.2 and Corollary 3.2 we can construct QMDS codes systematically from classical codes over composite alphabets, for example, families of RS codes. Especially, when $\mathcal{A} = \mathrm{GF}(p^m)$, it is possible to construct QMDS codes from DERS and TERS codes. First, from two DERS codes with parameters $[p^m+1, k_1, p^m-k_1+2]_{p^m}$ and $[p^m+1, k_2, p^m-k_2+2]_{p^m}$ where $k_1 \geq k_2$, $k_1+k_2 = p^m+1$, and $k_1-k_2 = k$, we obtain a $[[p^m+1, k, (p^m-k_1+3)/2]]_{p^m}$ quantum doubly-extended RS (QDERS) code.

Corollary 3.3. *There exists a QDERS code with parameter* $[[p^m+1, k, (p^m-k+3)/2]]_{p^m}$ *for* $0 \leq k \leq p^m+1$.

It is possible to obtain QMDS codes with parameters in the above corollary from cyclic MDS codes with parameters $[p^m+1, k, p^m-k+2]_{p^m}$ for $1 \leq k \leq p^m+1$ in the same way [15]. Next, there exist two TERS codes with parameters $[2^m+2, 3, 2^m]_{2^m}$ and $[2^m+2, 2^m-1, 4]_{2^m}$ and from them we also obtain a $[[2^m+2, 2^m-4, 4]]_{2^m}$ quantum triply-extended RS (QTERS) code.

Corollary 3.4. *There exists a QTERS code with parameter* $[[2^m+2, 2^m-4, 4]]_{2^m}$.

From the CSS construction over finite fields several families of quantum codes were constructed including quantum Reed-Solomon codes (QRS) [24, 14, 15] and quantum Reed-Muller (QRM) codes [4, 16] which are derived from RS codes and Reed-Muller (RM) codes, respectively. Especially, in the previous paper [14], we defined a series of families QRS codes as follows: We called quantum codes, obtained from a GRS code and an ERS code, a quantum generalized Reed-Solomon (QGRS) code and a quantum extended Reed-Solomon (QERS) code, respectively. The above QDERS codes and QTERS codes are defined in the same way. Theorem 3.2 also gives $[[p^m-1, k, (p^m-k+1)/2]]_{p^m}$ quantum generalized RS (QGRS) codes and $[[p^m, k, (p^m-k+2)/2]]_{p^m}$ quantum extended RS (QERS) codes in [15, 14].

In addition to RS codes, RM codes can also be used in the construction of QMDS codes. Recently, quantum RM codes over finite fields, which are also QMDS, were introduced in [16].

We can also apply Theorem 3.2 to RS codes over composite alphabets as in the following corollary.

Corollary 3.5. *(QMDS Codes by Coadunate RS Codes) If there exist* n *such that* $n = p_j^{m_j} + a_j$ *where* $a_j = -1, 0, 1, 2$ *and* p_j*'s are primes for* $j = 1, 2, \ldots, l$*, then there exists a QMDS code with parameter* $[[n = p_j^{m_j} + a_j, k, (n-k+2)/2]]_{\prod_{j=1}^{l} p_j^{m_j}}$ *code.*

Proof. Consider two coadunate RS codes with parameters $[[n = p_j^{m_j} + a_j, k_1, (n-k_1+2)/2]]_{\prod_{j=1}^{l} p_j^{m_j}}$ and $[[n = p_j^{m_j} + a_j, k_2, (n-k_2+2)/2]]_{\prod_{j=1}^{l} p_j^{m_j}}$ for $k_1 > k_2$. If $k_1 + k_2 = n$ and $k_1 - k_2 = k$, then by Theorem 3.2 we obtain an $[[n = p_j^{m_j} + a_j, k, (n-k+2)/2]]_{\prod_{j=1}^{l} p_j^{m_j}}$ quantum RS code. □

By the same argument as that in the last paragraph of Section 3.1, we can obtain infinitely many QMDS codes through Corollary 3.5.

3.3 Quantum Coadunate MDS Codes

From now on we will deal with a method to conjoin QMDS codes over any alphabets into a QMDS code over direct sum of the alphabets.

Quantum codes with the same length can be linked together to bring in a quantum coadunate code over a composite alphabet. The following lemma is a quantum analogue of Lemma 3.1, and is an extension of the result in [10] where a quantum error-correcting code over a composite alphabet is obtained from quantum codes with the same length and distance.

Lemma 3.2. *(Quantum Coadunate Code) If there exist* $((n, K_j, d_j))_{q_j}$ *codes over* q_j*-dimensional systems for* $j = 1, 2, \ldots, l$*, then there also exists an* $((n, \prod_{j=1}^{l} K_j, d))_{\prod_{j=1}^{l} q_j}$ *code where* $d = \min\{d_1, d_2, \ldots, d_l\}$.

We next state a necessary and sufficient condition for a quantum coadunate code to be MDS, which is a quantum version of Theorem 3.1 and can be proved in a similar way to Theorem 3.1.

Theorem 3.3. *(Quantum Coadunate MDS Code) Suppose that an* $((n, \prod_{j=1}^{l} K_j, d))_{\prod_{j=1}^{l} q_j}$ *code* $\mathcal{C}$ *is constructed by* $((n, K_j, d_j))_{q_j}$ *codes* $\mathcal{C}_j$ *over* $\mathcal{A}_j$ *for* $j = 1, 2, \ldots, l$*.* $\mathcal{C}$ *is QMDS if and only if* $\mathcal{C}_j$ *codes are all QMDS and satisfy that* $K_1 = K_2 = \cdots = K_l$ *and* $d_1 = d_2 = \cdots = d_l$.

QMDS codes over finite fields satisfying the assumptions in Theorem 3.3 can combine to form a QMDS code over a composite alphabet. Up to now several families of QMDS codes over Galois fields have been developed and are listed in Table 1. By joining QMDS codes in Table 1 together we can obtain new classes of QMDS codes some examples of which are listed in Table 2. QMDS codes with parameters (A) are CSS codes constructed by DERS and TERS codes in Section 3.2, and they belong to the family of quantum RS codes with parameters (L). All but quantum codes with parameters (A) are QMDS codes over the direct sum of finite fields and are obtained by applying Theorem 3.3 to QMDS codes with parameters in Table 1 and with parameters (A) in Table 2. Especially, QMDS codes with parameters (B), (C), (D), and (E) are constructed by merging quantum codes with parameter (a), (c), (d), and (e) with themselves, respectively. QMDS codes with the rest parameters are the joints of heterogeneous QMDS codes. In a detail account, quantum coadunate codes with parameters (L) are obtained by conjoining quantum RS codes with parameters (f) and (A) such that $n = p_j^{m_j} + a_j$ for $j = 1, 2, \ldots, l$. We remark that these coadunate codes are equivalent to CSS codes obtained from classical coadunate RS codes in Corollary 3.5. As explained in the last paragraph of Section 3.1, one can find infinitely many families of quantum coadunate RS codes satisfying the conditions in Theorem 3.3. Quantum RM codes together with quantum RS codes permit wider range of code lengths as shown in parameters (K). We note that although QMDS codes with parameters (F),(G),(H), and (I) defined over alphabets, the sizes of which are powers of primes, they are not defined over finite fields.

Table 1: Parameters in previous QMDS codes

Index	Parameters
(a)	$[[n, n, 1]]_2$ for $n \geq 1$, $[[n, n-2, 2]]_2$ for even n, $[[5, 1, 3]]_2$, and $[[6, 0, 4]]_2$ in [11]
(b)	$[[5, 1, 3]]_q$ for a positive integer q in [12]
(c)	$[[p^{2m}+1, p^{2m}-3, 3]]_{p^m}$ and $[[p^{2m}, p^{2m}-4, 3]]_{p^m}$ in [13]
(d)	$[[n, k, (n-k+2)/2]]_{p^m}$ for $3 \leq n \leq p^m$ and $[[p^{2m}-s, k, (p^{2m}-s-k+2)/2]]_{p^m}$ for some s and $1 \leq d \leq p^m$ in [15]
(e)	$[[p^{2m}, p^{2m}-2\nu-2, \nu+2]]_{p^m}$ and $[[(\nu+1)p^m, (\nu+1)p^m-2\nu-2, \nu+2]]_{p^m}$ for $0 \leq \nu \leq p^m-2$ in [16]
(f)	$[[p^m-1, k, (p^m+1-k)/2]]_{p^m}$ and $[[p^m, k, (p^m+2-k)/2]]_{p^m}$ in [14]

3.4 Quantum Puncturing and Shortening

The lengths of most error-correcting codes over finite fields are restricted depending on the sizes of alphabets. As a partial solution to this problem, there exist two methods quantum puncturing [10] and shortening [8] over finite fields which enable us to construct quantum stabilizer codes with shortened lengths. Especially, if a QMDS code is given, then we can obtain QMDS codes with shortened lengths by using the methods. We will show that it is possible to extend these methods over composite alphabets.

First, let us explain quantum puncturing over composite alphabets in short. Let $C \subset (\mathcal{A} \times \mathcal{A})^n$ be of length n and dimension $n-k$ code such that $C^\perp$ has the distance d. For any pair, $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{c}, \mathbf{d})$ in C, we define a vector in $\mathcal{A}^n$ by $\{(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d})\} = (\langle\langle(\mathbf{a}^{(1)}, \mathbf{b}^{(1)}), (\mathbf{c}^{(1)}, \mathbf{d}^{(1)})\rangle\rangle_q, \langle\langle(\mathbf{a}^{(2)}, \mathbf{b}^{(2)}), (\mathbf{c}^{(2)}, \mathbf{d}^{(2)})\rangle\rangle_q, \ldots, \langle\langle(\mathbf{a}^{(n)}, \mathbf{b}^{(n)}), (\mathbf{c}^{(n)}, \mathbf{d}^{(n)})\rangle\rangle_q)$ where $\langle\langle(\mathbf{a}^{(i)}, \mathbf{b}^{(i)}), (\mathbf{c}^{(i)}, \mathbf{d}^{(i)})\rangle\rangle_q = \sum_{j=1}^{l} \sum_{k=1}^{m_j} (\mathbf{a}_{ijk}\mathbf{d}_{ijk} - \mathbf{b}_{ijk}\mathbf{c}_{ijk})\hat{p_j}$. The puncture code $P(C)$ of C is defined by the dual code of the code generated by all $\{(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d})\}$ with respect to the usual inner product on $\mathcal{A}^n$. If there exists a codeword in $P(C)$ that has $n-s$ components, each of which consists of non-zero elements, then there exists a stabilizer code $\mathcal{C}$ with parameter $[[n-s, k'-s, d']]_q$ for $k' \geq k$ and $d' \geq d$. If C corresponds to a QMDS code with parameter $[[n, k, d]]_q$, then $\mathcal{C}$ is also an $[[n-s, k-s, d]]_q$ QMDS code by the Singleton bound.

On the other hand, quantum shortening is carried out by removing a column containing two non-commutative operators and the corresponding two rows in a generator matrix of a stabilizer group. If a generator matrix of a stabilizer group of an $[[n, k, d]]_q$ QMDS code has a column containing two non-commutative elements, then there also exists a QMDS code with parameter $[[n-1, k+1, d-1]]_q$.

Whereas quantum puncturing is bound to preserve the code distance and lower

Table 2: Some examples of parameters in new QMDS codes; Indices in the construction column mean the parameters of quantum codes conjoined into QMDS codes over composite alphabets. For example, (e)+(A) means that a QMDS code is constructed from QMDS codes with parameter (e) in Table 1 and QMDS codes with parameter (A) in this table.

Index	Construction	Parameter
(A)	DERS	$[[p^m+1, k, (p^m+3-k)/2]]_{p^m}$ (QDERS codes)
	TERS	$[[2^m+2, 2^m-4, 4]]_{2^m}$ (QTERS codes)
(B)	(a)+(a)	$[[n, n, 1]]_{2^m}$ for $n \geq 1$, $[[n, n-2, 2]]_{2^m}$ for even n, and $[[6, 0, 4]]_{2^m}$
(C)	(c)+(c)	$[[p^{2c}+a, p^{2c}+a-4, 3]]_{p^m}$ for $a = 0, 1$ and $c \mid m$
(D)	(d)+(d)	$[[p^{2c}-s, p^{2c}-s-2d+2, d]]_{p^m}$ for some s, $1 \leq d \leq p^c$, and $c \mid m$
(E)	(e)+(e)	$[[p^{2c}, p^{2c}-2\nu-2, \nu+2]]_{p^m}$ and $[[(\nu+1)p^c, (\nu+1)p^c-2\nu-2, \nu+2]]_{p^m}$ for $0 \leq \nu \leq p^c-2$ and $c \mid m$
(F)	(e)+(f)	$[[p^{(m+c)/2}, p^{(m+c)/2}-2p^c, p^c+1]]_{p^m}$ for $0 \leq c \leq m/3$
(G)	(c)+(f)	$[[p^{2m/3}, p^{2m/3}-4, 3]]_{p^m}$
(H)	(c)+(A)	$[[p^{2m/3}+1, p^{2m/3}-3, 3]]_{p^m}$
(I)	(d)+(f) or (d)+(A)	$[[p^{2m/3}-s, k, (p^{2m/3}-s-k+2)/2]]_{p^m}$ for some $s \geq 0$ and $[[p^c+a, k, (p^c+a-k+2)/2]]_{p^m}$ for $2c \leq m$ and $a = -1, 0, 1, 2$
(J)	(c)+(e)	$[[n = p_1^{2m_1}+1 = (\nu+1)p_2^{m_2}, k, (n-k+2)/2]]_{p_1^{m_1}p_2^{m_2}}$ for $0 \leq \nu \leq p_2^{m_2}-2$
(K)	(e)+(f) or (e)+(A)	$[[n = (\nu+1)p_1^{m_1} = p_2^{m_2}+a, k, (n-k+2)/2]]_{p_1^{m_1}p_2^{m_2}}$ for $0 \leq \nu \leq p_1^{m_1}-2$ and $a = -1, 0, 1, 2$
(L)	(f)+(A)	$[[n = p_j^{m_j}+a_j, k, (n-k+2)/2]]_{\prod_{j=1}^{l} p_j^{m_j}}$ for $a_j = -1, 0, 1, 2$ and prime p_j

the code dimension, quantum shortening shortens the code distance and makes higher dimensional QMDS codes than original ones. That is, although both of them derive QMDS codes with shortened lengths, the former pursues the correction of more errors and the latter pursues the efficiency of sources.

In classical error-correcting codes, MDS codes with shortened length n' satisfying $d \leq n' \leq n$ can always be constructed from an $[n, k, d]$ MDS code [27]. However, quantum puncturing and shortening do not guarantee the existence of QMDS codes for all shortened lengths because the orthogonality with respect to the weighted symplectic inner product should be preserved. In the last section, we presented a practical method to merge QMDS codes over finite fields into QMDS codes over direct sums of finite fields and this method guarantees QMDS codes over alphabets of size p^m with shortened lengths. Thus the conjoining method can be another complementary solution to construct QMDS codes with shortened lengths, as shown in Table 2.

4 Conclusion

In this paper, we diversified not only the dimension of quantum system applicable to quantum error-correcting codes, but also broadened the range of lengths of quantum codes for given sizes of alphabets by constructing quantum coadunate codes . To deal with quantum codes over composite alphabets, we identified alphabets with commutative rings instead of the conventional finite fields. Based on the ring structure of an alphabet, we constructed a unitary operator basis and then generalized the non-binary quantum stabilizer construction and extended the CSS construction. Especially, self-orthogonal classical codes with respect to the weighted inner product represent quantum stabilizer codes. Moreover, we used the coadunate method to construct error-correcting codes over composite alphabets and presented a necessary and sufficient condition for coadunate codes to be MDS. Under this condition, we could compose infinitely many families of MDS and QMDS codes over alphabets of arbitrary size. Especially, by the CSS construction we constructed quantum coadunate RS (and MDS) codes including QDERS and QTERS codes.

Acknowledgement

This work was supported by AFOSR/AOARD under grant FA5209-04-P-0228 (AOARD-044-010).

References

[1] P. W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A **52** (1995), 2493–2496.

[2] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exits*, Phys. Rev. A **54** (1996), 1098–1105.

[3] A. M. Steane, *Multiparticle interference and quantum error correction*, Proc. Roy. Soc. Lond. A **452** (1996), 2551–2577.

[4] A. M. Steane, *Quantum Reed-Muller codes*, IEEE Transactions on Information Theory **45** (1999), 1701–1703.

[5] E. Knill and R. Laflamme, *Concatenated quantum codes,* Los Alamos e-print archive, quant-ph/9608012 (1996).

[6] M. Grassl and T. Beth, *Cyclic quantum error-correcting codes and quantum shift registers*, Los Alamos e-print archive, quant-ph/9910061 (1999).

[7] E. Knill and R. Laflamme, *A theory of quantum error-correcting codes*, Phys. Rev. A **55** (1997), 900–911.

[8] D. Gottesmann, *Stabilizer codes and quantum error correction*, Los Alamos e-print archive, quant-ph/9705052 (1997) (Caltech Ph.D. Thesis).

[9] D. Gottesmann, *An introduction to quantum error correction*, Los Alamos e-print archive, quant-ph/0004072 (2000).

[10] E. M. Rains, *Nonbinary quantum codes,* IEEE Transactions on Information Theory **45** (1999), 1827–1832.

[11] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, *Quantum error correction via codes over GF(4)*, IEEE Transaction on Information Theory **44** (1998), 1369–1387.

[12] H. F. Chau, *Five quantum register error correction code for higher spin system*, Phys. Rev. A **56** (1997), R1–R4.

[13] J. Bierbrauer and Y. Edel, *Quantum twisted codes*, Journal of Combinatorial Designs 8 (2000), 174–188; The paper is available at "http://www.math.mtu.edu/ jbierbra/".

[14] D. P. Chi, J. Kim, J. Lee and S. Lee, *QMDS Codes*, manuscript, presented at KIAS Workshop on Quantum Computation and Quantum Information, Seoul, Korea, 2001.

[15] M. Rötteler, M. Grassl and T. Beth, *On QMDS codes,* Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on 27 June-2 July, 2004, 356–356. M. Grassl and T. Beth, *On optimal quantum codes,* Los Alamos e-print archive, quant-ph/0312164 (2003).

[16] P. K. Sarvepalli and A. Klappenecker, *Nonbinary quantum Reed-Muller codes*, Los Alamos e-print archive, quant-ph/0502001 (2005).

[17] E. Knill, *Non-binary unitary error bases and quantum codes,* Los Alamos e-print archive, quant-ph/9608048 (1996).

[18] E. Knill, *Group representations, error bases and quantum codes,* Los Alamos e-print archive, quant-ph/9608049 (1996).

[19] H. F. Chau, *Correcting quantum errors in higher spin system*, Phys. Rev. A **55** (1997), R839–R841.

[20] R. Cleve, *Quantum stabilizer codes and classical linear codes*, Phys. Rev. A **55** (1997), 4054–4059.

[21] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, *Quantum error correction and orthogonal geometry*, Phy. Rev. Lett. **78** (1997), 405–408.

[22] A. Ashikhmin and E. Knill, *Nonbinary stabilizer codes,* Los Alamos e-print archive, quant-ph/0005008 (2000).

[23] D. Aharonov and M. Ben-or, *Fault-tolerant quantum computation with constant error*, Proceedings of the 29th Annual ACM Symposium on Theory of Computing, Association for Computing Machinery, 1997, 176–188. Los Alamos e-print archive, quant-ph/9611025 (1996).

[24] M. Grassl, W. Geiselmann and T. Beth, *Quantum Reed Solomon codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes(AAECC-13),(1999). Lecture Notes in Computer Science **1719** Springer-Verlag (1999), 231–244.

[25] Forney, G. D. Jr. *On the Hamming distance properties of group codes*, Information Theory, IEEE Transactions 38 (1992), 1797–1801.

[26] L. M. G. M. Tolhuizen, *On maximum distance separable codes over alphabets of arbitrary size*, Information Theory, 1994 Proceedings, 1994 IEEE International Symposium on 27 June-1 July, 1994, 431–431.

[27] F. J. Macwilliams and N. J. A. Sloane, *The theory of error correcting codes,* North-Holland, 1977.

[28] G. Seroussi and R. M. Roth, *On MDS extensions of generalized Reed-Solomon codes*, IEEE Transactions on Information Theory **32** (1986), 349–354.

[29] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed. Oxford, England: Clarendon Press, 1979.